PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 — A1

(11) International Publication Number: WO 97/44736

(43) International Publication Date: 27 November 1997 (27.11.97)

(21) International Application Number: PCT/US97/08264

(22) International Filing Date: 15 May 1997 (15.05.97)

(30) Priority Data:
08/652,862 23 May 1996 (23.05.96) US

(71) Applicant: APPLE COMPUTER, INC. [US/US]; 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

(72) Inventor: WEHRENBERG, Paul, J.; 3516 Ross Road, Palo Alto, CA 94303 (US).

(74) Agents: CARMICHAEL, Paul, D. et al.; Apple Computer, Inc., 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

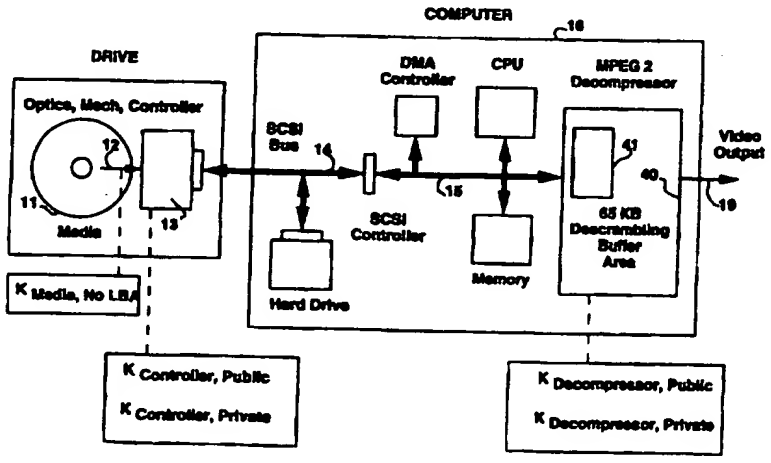
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION



(57) Abstract

An apparatus and method for providing two levels of copy protection, including a first method for copy protection, including a key, and a second method for copy protection. One level of copy protection is a moderately secure level to allow decrypting a medium- to high-bandwidth data stream without significant delay of the data stream. The second level of copy protection can be highly secure but can be utilized less often and so can be decrypted more slowly. One useful combination is to use a key encryption scheme for the first level of copy protection of a primary data stream, then to use the second protection scheme to securely transfer the first level key from a protected storage location to a decoding location. Encoded primary data can be stored on a removable media, together with the decryption key stored in a special location. The media drive unit can access the special location and, using the second level copy protection scheme, transfer the key securely to a descrambling unit. The first level copy protection can involve selective reordering of data subunits within a data unit according to a scrambling vector, then encoding the scrambling vector using the first key, and storing the encoded scrambling vector with the corresponding data unit.

METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION

Field of the Invention

This invention relates to data encryption and decryption, and more particularly to an improved method and apparatus for using one level of encryption to establish a secure communication channel, then passing a decryption key over that channel for subsequent decryption. This invention includes a new method of scrambling bulk data. This invention is particularly useful for protecting bulk information intended for widespread distribution such as movies or music in CD or DVD formats.

Background of the Invention

The field of data encryption has been the subject of extensive scholarly investigation and has been the topic of many patents in the United States and other countries. For general reference, the background description in each of United States Patent Nos. 5,497,422 (Tysen et al., 5 March 1996) and 5,438,622 (Normile et al., 1 August 1995) discuss representative encryption schemes known in the art. Each of these patent applications are assigned to Apple Computer, Inc. These patents are incorporated herein by reference in their entirety.

A wide variety of information is sold to consumers in various forms. One major category of information is computer software. Another major category of information is music, often in the form of CDs or tape. Still another major category of information is movies, usually over cable or satellite television links but often in the form of analog tape or LaserDisc. There is a tension in distribution of any form of information because if consumers will buy it from a rightful owner, other consumers are likely to buy illegal copies made from legitimate originals.

Various copy protection schemes have been considered for use with various media. Scrambling of cable or satellite channels is common. A variety of anti-copying schemes are used in analog video tape. CDs or digital tape can be encoded with anti-copying codes.

Distribution of various information in digital form has troubled many content providers because making the information available potentially makes it quite simple for a user to make one or many illegal copies of that content. Forms of such content include movies, music, and data such as encyclopedic

One stage of the retrieval system includes an encryption scheme to assure that the retrieval is made in an authorized system, and another stage of the retrieval system uses a stored encryption key to decode the data of interest. In one preferred implementation, the encryption key is used as a descrambling code.

To minimize the performance impact on the apparatus and not constrain use of system resources by low priority or low value data streams, the information flow can be broken into elements with a distinct hierarchy of bandwidth. For example, an MPEG stream (high bandwidth) may be merely scrambled, the scrambling control bits (much lower bandwidth) may be encoded, and only the MPEG-decode key information necessary to decode the scrambling control bits (very low bandwidth) is key encrypted.

The scrambling can be done in any of many ways, some of which are discussed in detail below. For example, the order of the data within a unit of data can be reordered in a controlled way to give a scrambled signal. Each unit of data, such as a 64 KB block, can be scrambled in a defined way, then a descriptor which characterizes that scrambling can be encrypted using a key and the encoded descriptor can be stored with the relevant block of data. A single key can be used to decrypt any scrambling descriptor and the descriptor can be changed for each unit of data, that is, each unit of data can be independently scrambled. With a key available, it is relatively straightforward to correctly reorder the scrambled data into the original, "clear text" format. With no key, if a sufficiently complex scrambling method has been chosen, it can be challenging to identify the correct key by trial and error, particularly since each data unit is scrambled in a different pattern. With the key, a moderately complex scrambling method will not have a significant effect on data reconstruction rate and thus becomes transparent to the user.

This copy protection becomes much more powerful if the key can be changed for different units of primary information, for example for each movie title.

Storage and access to this key raises an interesting challenge, but this can be managed very conveniently by using a separate encryption mode to secure the key and provide it in a coordinated fashion with the program of interest. One way to do this is to store the key in a secure manner on the same storage medium as the scrambled information. The mechanism of this separate storage mode can be set at a desired level of complexity. One preferred mode is to make this key inaccessible by typical access operations, but readily accessible through special operations. Specifically, in just one preferred embodiment, the

Moving the implementation burden on the computer system toward the peripheries, i.e. the media, the mass storage device, and the application software minimizes the impact on the operating system software and motherboard hardware. This method and apparatus avoids the need to create new high bandwidth information flow paths and new file systems while providing useful protection for the valuable source information.

One object of this invention is to provide reasonably effective prevention of casual copying by a user.

Another object of this invention is to provide a copy protection scheme with little or no impact on or modification of the traditional, primary computer components.

Still another object of this invention is to minimize the performance impact of the protection scheme by selectively protecting the most unique or most valuable portions of a data stream.

This and other objects and advantages of the invention, as well as the details of an illustrative embodiment, will be more fully understood from the following specification and drawings.

Brief Description of the Drawings

Figure 1 illustrates an apparatus useful in practicing this invention.

Figures 2A, 2B and 2C illustrate a source data structure in its original form (2A), then formatted and addressed after scrambling (2B) and then formatted and addressed after encrypting the scrambling vector (2C).

Figure 3 illustrates encryption of a 32 element scrambling vector.

Figure 4 illustrates descrambling inside an MPEG2 decoder.

Description of the Preferred Embodiments

Representative elements and the process of a preferred implementation of the copy protection scheme are described below. A preferred embodiment will be described by way of example. Figure 1 gives a schematic of the complete system. Note that the MPEG decoder is depicted as a hardware element, but the copy protection method can be used, perhaps with a lesser degree of protection, when the MPEG decoder is a software process. A more generic system includes only a medium, a reader for that medium, a destination for information from that medium, and a channel between the reader and the destination.

The medium does not need to be physically close to the destination. For example, the source information might be stored on a server such as a video-

secure channel between the reader, for example the device where the primary key is maintained, and the destination, for example the device where the primary key is to be used.

As illustrated in Figure 1, there are five keys involved in one preferred implementation of the copy protection apparatus of this invention, one for the primary information and four for secure transfer of that key.

Secure Transfer of the Primary Information Key

In one preferred embodiment, the primary information key is placed on the media during manufacture. It may be stored in a location or sub channel that is readily accessible to the drive controller but difficult or impossible to access otherwise. In a preferred embodiment, is not in an area that is addressable by logical block address (LBA) and thus is not accessible by devices other than the drive controller itself. This primary information key is transferred as the message for a public key/private key transaction through the open computer system to a descrambler where it is used to descramble the primary information.

The drive controller is possessed of a public key and a private key, and has the capability of receiving another entity's public key. The drive can then encrypt a message using its private key and the received public key. This encrypted message can be requested by the operating system and passed to the owner of the non-drive public key, the destination.

The non-drive entity can then use its own private key and the drive's public key to decrypt the received message. As noted above, the key on the media is the message for the second encoding system. Thus the key for the primary encoding is itself encoded using the second encoding system and transferred through the open computer system to the non-drive entity, where it is decoded according to the second encoding scheme. This key can then be loaded into the primary decoding system and used directly.

The key encoding transaction described above uses very robust encryption which may be computationally intensive. However the size of the message is small and the transaction is a one time thing which is done at startup. The complexity of this encryption allows for a very high level of security. Since this encryption and decryption take place infrequently, preferably only at startup, there is very little penalty to taking some time. A typical user will not mind and may not even notice a delay of up to even a few

installed MPEG2 decoders. The operating system obtains public keys from drive 10 and MPEG2 decoder 40 (if present). The operating system provides the public key of the decoder 40 to the drive 10 and public key of the drive 10 to the decoder 40. The DVD-ROM device driver refuses to accept any MPEG decoder public key except during the startup sequence. This give some extra security against impersonation.

Use of the Primary Information Key

During primary data transfer operation, the primary information key is used by the recipient, e.g. the MPEG decoder, to correctly reorder the scrambled logical blocks received by streaming off of the storage device, e.g. a DVD disk. The specific function of the primary information key depends on the specific scrambling scheme. One preferred scrambling scheme is described below. Once transferred to the recipient, the primary information key is inserted into an appropriate decoder, then used to unscramble the primary data stream. In a preferred embodiment, the primary data stream is scrambled MPEG data which is descrambled to give a traditional MPEG data stream which then is decoded to give a video image, for example, an NTSC standard image or an RGB image, which can be displayed on an appropriate monitor.

Scrambling Scheme

The preferred scrambling scheme is designed to be computationally intensive to break if attacked as a jig saw puzzle, but easy to reorder if the key is available. A data unit is divided into smaller units, which are then rearranged according to a selected scheme. Information for reordering that data unit is stored for retrieval in conjunction with that data unit. This might take the form of a scrambling vector, which might be stored in a subheader or perhaps embedded in the scrambled data unit. The information can be further protected by encoding the scrambling vector according to an encryption scheme, using a selected primary information key. The same process can be repeated for subsequent data units, but each data unit can be rearranged in a different order. In each instance, the scrambling vector is retrievable and can be reassociated with its corresponding data unit. The same primary information key can be used to encode a series of scrambling vectors. The primary information key, along with each particular instance of the encoded

reversible algorithm whose parameters are defined by the media key, K_{Media}. Recall this is the key that is only readable by the drive 10, and this key is never passed as clear text through the open system. There are a number of simple approaches available for encrypting the scrambling vector, such as tapped shift registers, pseudo random sequence generators, etc.

Referring to Figure 4, descrambling is done inside MPEG2 decoder 40. The descrambling buffer area 41 is equal to or greater than the 64 KB of user data plus the 32 byte overhead of the SV*. Typical memory allocation might be done on 1 KB boundaries, so handling the SV* and converting it back to SV might necessitate 65 KB for the descrambling buffer area. The internal output is a clear text MPEG data stream which is then decoded to give final output 19 as uncompressed video.

Other data streams can be processed in an analogous manner.

Another preferred scrambling scheme reorders only part of the user data block. An MPEG data stream includes high order bits that define information about the sequence of the user data blocks. If data blocks including this information were simply reordered, it would be possible to use those specific bits to reassemble the data in the correct order. However, if only part of the user block is reordered and the expected sequence information is left untouched, the user blocks will be corrupted because the first part of the user block will be matched with the second part of a different user block. In a preferred implementation, the first half of each block is untouched while the second half of each block is reordered as described above in connection with Figures 2A, 2B and 2C. The scrambling vector is prepared, encoded and stored as described above. This scheme still has 32! possible combinations. Since each data unit can be reordered using a different scrambling vector, descrambling will be difficult without the key, but simple with the correct primary information key.

The size of the data unit affects the complexity of encoding and decoding. The example above describes a data unit subdivided into 32 blocks. This allows reordering in 32! possible combinations which gives a fairly complex, and thus secure, encoding scheme. In the DVD specification, a standard data unit is 32 KB of 2 KB subunits. This provides 16 blocks which can be reordered as decribed above, to give 16! possible combinations of scrambled data.

A media drive controller can be designed to support this scheme at minimal cost impact. As far as the transferring a scrambled primary data stream, a traditional drive controller need not be modified at all. To support

Claims

What is claimed is:

1. An apparatus for providing two levels of copy protection, said apparatus comprising

first means for copy protecting information, said first means including a key, and

second means for copy protecting information, said second means applied to said key for said first means.

2. The apparatus of claim 1 wherein said first means for copy protecting information is a selective disordering of an information data stream and said key can be used to correctly reorder the disordered information data stream.

3. The apparatus of claim 1 further comprising two devices connected by a communication channel and wherein said second means for copy protecting information is a means to provide a secure communication channel between two devices.

4. The apparatus of claim 3 wherein said second means for copy protecting information includes use of a public and private key by at least one of said two devices.

5. The apparatus of claim 3 wherein said key for said first means for copy protecting information is encoded for transmission over said communication channel between said two devices.

6. The apparatus of claim 1 further comprising

a source of information encoded according to a first means for copy protection,

a decoder for said information according to said first means for copy protection, using said key,

a storage location for said key,

a means for communicating between said storage location and said decoder,

wherein said second means for copy protecting information comprises means for encoding said key for secure communication between said storage location and said decoder.

LBA n	2 KB User Data (block n)
LBA n + 1	2 KB User Data (block n + 1)
LBA n + 2	2 KB User Data (block n + 2)
LBA n + 3	2 KB User Data (block n + 3)
LBA n + 4	2 KB User Data (block n + 4)
LBA n + 5	2 KB User Data (block n + 5)
LBA n + 31	2 KB User Data (block n + 31)

FIGURE 2A

LBA n	SVE 0 (5)	2 KB User Data (block n + 5)
LBA n + 1	SVE 1 (31)	2 KB User Data (block n + 31)
LBA n + 2	SVE 2 (17)	2 KB User Data (block n + 17)
LBA n + 3	SVE 3 (4)	2 KB User Data (block n + 4)
LBA n + 4	SVE 4 (24)	2 KB User Data (block n + 24)
LBA n + 5	SVE 5 (0)	2 KB User Data (block n)
.....	.....	.....
.....	.....	.....
LBA n + 31	SVE 31 (22)	2 KB User Data (block n + 22)

FIGURE 2B

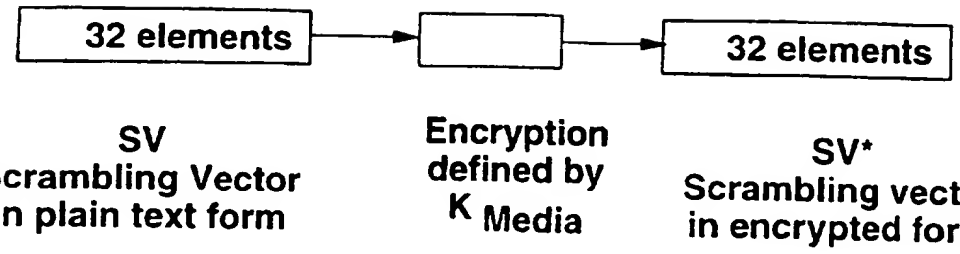


FIGURE 3

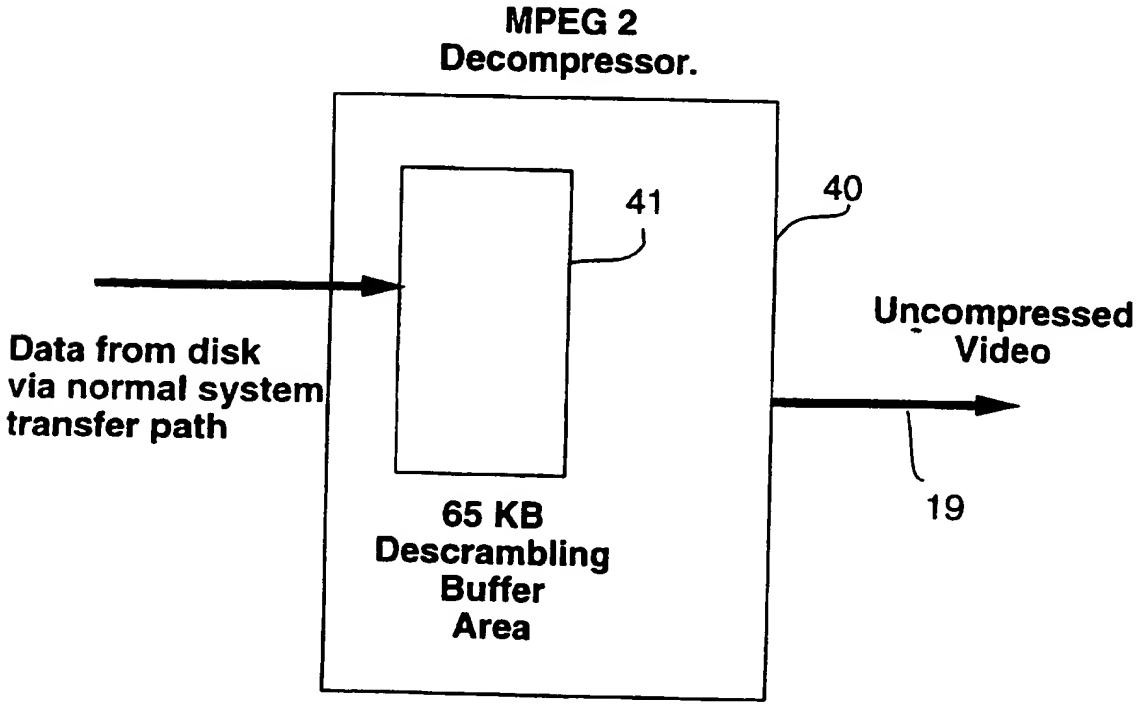


FIGURE 4